Remarks

Claim 22 has been amended as to form in response to the criticism in the Official Action.

Claims 1-3, 5, 14-21, 31, 34, and 39 were rejected under §112, second paragraph, for including "adapted to." These claims have been amended and reconsideration and withdrawal of the rejection are respectfully requested. However, it is noted that "adapted to" can be acceptable for a patentable limitation. See, for example, MPEP §2111.04 that states that this phrasing can define a patentable limitation, depending on whether it is clear the that the intention is to use the phrase to define a patentable limitation (see also §2173.05(g) and §2181 I). While it is believed that use of "adapted to" in the claims is clearly intended to define a patentable limitation, the claims have been amended in a manner intended to improve their clarity.

Claims 1-6, 8-23, 25-37, and 39-41 were rejected as anticipated by CHEFALAS et al. 2002/0116639. The independent claims have been amended and reconsideration and withdrawal of the rejection are respectfully requested.

The amended claims define a security system and method in which a first sub-system detects unknown malicious softwares having one or more characteristics unknown to the first sub-system, the first sub-system being configured to perform at least a partial simulation to activate unknown malicious softwares having one or more characteristics unknown to the first sub-

system and to detect the activated unknown malicious softwares by detecting consequences of activation of the unknown malicious softwares.

CHEFALAS et al. disclose (paragraph 0012) a software subsystem (VSN) and/or software module (VSC) in which the VSN sends a virus notification to the VSC and the VSC send a virus-detected event and an email message to a remote administrator (paragraph 0030). In one option, the VSN is capable of detecting viruses on the basis of known features of viruses (paragraph 0030), while in another option the VSC is capable of detecting viruses on the basis of known features of viruses (paragraph 0031). In both options, the VSN/VSC is a traditional virus scanner detecting viruses on the basis of an updateable virus database that includes identification data for each known virus (paragraphs 0012, 0031). That is, nothing in CHEFALAS et al. is simulated, rather the virus scanners of both the VSN and VSC detect viruses using virus databases that include feature of known viruses.

By way of further explanation, CHEFALAS et al. use a traditional anti-virus program to look for known viruses. These traditional anti-virus programs run are run constantly as so-called background processes. They are operated in connection with starting of a computer at least partially in the working storage to control data transfer between the information network and the computer, the internal operation of the computer, and the

contents of mass storage. The anti-virus programs usually contain a database of characteristics of known viruses. When a new file is saved in the working storage of the computer, the anti-virus software compares the information to the characteristics of known viruses. The database must be updated to be useful.

Polymorphic viruses can transform themselves in connection with copying and are thus particularly difficult to detect using traditional anti-virus programs. The mutations of the polymorphic viruses may contain the same virus functions, but traditional database anti-virus programs can not be relied upon to identity the mutations. By contrast, the invention defined in the present claims searches messages for viruses unknown to the detecting device using a simulation, and thus is able to detect the mutations.

CHEFALAS et al. do not disclose detection of unknown malicious softwares having one or more characteristics unknown to the detecting entity, where the entity is configured to perform at least a partial simulation to activate the unknown malicious softwares having the one or more characteristics unknown to the detecting entity, and to detect the activated unknown malicious softwares by detecting consequences of activation of the unknown malicious softwares.

In view of the present amendment and the foregoing remarks, it is believed that the present application has been

placed in condition for allowance. Reconsideration and allowance are respectfully requested.

The Commissioner is hereby authorized in this, concurrent, and future replies, to charge payment or credit any overpayment to Deposit Account No. 25-0120 for any additional fees required under 37 C.F.R. § 1.16 or under 37 C.F.R. § 1.17.

Respectfully submitted,

YOUNG & THOMPSON

/Thomas W. Perkins/

Thomas W. Perkins, Reg. No. 33,027
745 South 23rd Street
Arlington, VA 22202
Telephone (703) 521-2297
Telefax (703) 685-0573
(703) 979-4709

TWP/lk